EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"5745574".pn.	USPAT	OR	ON	2007/02/16 15:04
S2	1	"20040205344"	US-PGPUB	OR	ON	2007/02/16 11:50
S3	11	("5351293"|"5475757"|"5515111"|"5787169"|"6035405"|"6088450"|"6128742"|"6178508"|"6226383"|"6286104"|"6757825").PN.	USPAT	OR	ON	2007/02/08 10:35
S4	989	713/168,171.ccls. and (encrypt$ adj key)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 11:51
S5	204	713/168,169,171.ccls. and (key adj (encrypt$ adj key))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 11:52
S6	42	713/153-159,168-181.ccls. and (old adj certificate)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 15:08
S7	19	713/153-159,168-181.ccls. and ((replaced obselete) adj key)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 15:09
S8	133	713/153-159,168-181.ccls. and ((replaced obselete old) adj key)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/16 15:27

Sign in

Google Web Images Video News Maps more »

otway "trust authority" Search Advanced Search Preferences

Web Results **1 - 10** of about **201** for **otway "trust authority"**. (**0.27** seconds)

Information security subscriber **trust authority** transfer system ...
The second trusted authority serves as a new trust anchor instead of the first **trust authority**. Inventors:, **Otway**, Josanne;. Application Number:, 345234 ...
www.freepatentsonline.com/6192130.html - 72k - Cached - Similar pages

Information security subscriber **trust authority** transfer system ...
Information security subscriber **trust authority** transfer system with private key history transfer - US Patent 6192130 from ... Inventor(s). Josanne **Otway** ...
www.patentstorm.us/patents/6192130-claims.html - 33k - Cached - Similar pages

Information security subscriber **trust authority** transfer system ...
Inventor(s). Josanne **Otway** ... 1, a **trust authority**, such as a certification authority in a public key infrastructure, maintains private encryption key ...
www.patentstorm.us/patents/6192130-description.html - 57k - Cached - Similar pages

urn:schemas-microsoft-com:xml-sql 6105A320-9361-4471-80B2 ...
... such as Needham-Schroeder, **Otway**-Rees, Yahalom and Andrew Secure RPC. ... to avoid key escrow by a **Trust Authority** (TA) who issues identity based ...
csdl2.computer.org/comp/proceedings/csfw/2003/1927/00/1927toc.xml - 26k - Cached - Similar pages

專利- [Translate this page]
Information security subscriber **trust authority** transfer system with private key history transfer. Patent Number, US 6192130 (USA patent). Inventors, **Otway** ...
ics.stpi.org.tw/Patent/index.php?action=show&year=2001 - 450k - Cached - Similar pages

Information security subscriber **trust authority** transfer system ...
United States Patent, 6192130. **Otway**, February 20, 2001 ... 1, a **trust authority**, such as a certification authority in a public key infrastructure, ...
xrint.com/patents/us/6192130 - 67k - Supplemental Result - Cached - Similar pages

BigPatents -- Information security subscriber **trust authority** ...
Information security subscriber **trust authority** transfer system with private key history transfer ... Inventor. Josanne **Otway** Ottawa CAX ...
www.bigpatents.com/pnum/6192130 - 8k - Supplemental Result - Cached - Similar pages

esp@cenet document view
Information security subscriber **trust authority** transfer system with private ... Inventor:, **OTWAY** JOSANNE (CA). Applicant:, ENTRUST TECHNOLOGIES LTD (US) ...
v3.espacenet.com/textdoc?DB=EPODOC&IDX=US6192130&F=8 - 36k - Supplemental Result - Cached - Similar pages

[PDF] Section 1 Page 1 <a href="#2 ...
File Format: PDF/Adobe Acrobat
The **Otway** Health and Community Services ... Controlled **Trust Authority** Entity (Specific Trust defined in Authority Segment) ...
www.dtf.vic.gov.au/DTF/RWP323.nsf/0/ed753a11cc6e12dcca256dce0080ac81/$FILE/ATTRZC8U/AFRInfoManual.pdf - Similar pages

[PDF] An Architecture for Authorization and Delegation
File Format: PDF/Adobe Acrobat
Dave **Otway** and Owen Rees, "Efficient and timely mutual authentication", Operat- ... that the user directly trusts, and the **trust authority** TA ...
www.tml.tkk.fi/~pnr/publications/PhDThesis.pdf - Similar pages

Result Page: 1 2 3 **Next**

Published before July 2000
Terms used **encrypt old key previous key**

Found **66** of **113,315**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 66 Result page: **1** 2 3 4 next

Relevance scale

1 On simple and secure key distribution

Gene Tsudik, Els Van Herreweghen
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press

Full text available: pdf(702.78 KB) Additional Information: full citation, abstract, references, citings, index terms

The encrypted key exchange (EKE) protocol is augmented so that hosts do not store cleartext passwords. Consequently, adversaries who obtain the one-way encrypted password file may (i) successfully mimic (spoof) the host to the user, and (ii) mount dictionary attacks against the encrypted passwords, but cannot mimic the user to the host. Moreover, the important security properties of EKE are preserved—an active network attacker obtains insufficient information to mount dictionary attac ...

2 Secure group communications using key graphs

Chung Kei Wong, Mohamed Gouda, Simon S. Lam
February 2000 **IEEE/ACM Transactions on Networking (TON)**, Volume 8 Issue 1
Publisher: IEEE Press

Full text available: pdf(345.54 KB) Additional Information: full citation, references, citings, index terms, review

Keywords: confidentiality, group communications, group key management, key distribution, multicast, privacy, rekeying, security

3 Secure group communications using key graphs

Chung Kei Wong, Mohamed Gouda, Simon S. Lam
October 1998 **ACM SIGCOMM Computer Communication Review , Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '98**, Volume 28 Issue 4
Publisher: ACM Press

Full text available: pdf(1.68 MB) Additional Information: full citation, abstract, references, citings, index terms

Many emerging applications (e.g., teleconference, real-time information services, pay per view, distributed interactive simulation, and collaborative work) are based upon a group communications model, i.e., they require packet delivery from one or more authorized senders to a very large number of authorized receivers. As a result, securing group communications (i.e., providing confidentiality, integrity, and authenticity of messages delivered between group members) will become a critical network ...

4 Cryptanalysis of Microsoft's point-to-point tunneling protocol (PPTP)

Bruce Schneier, Mudge
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press
Full text available: pdf(1.02 MB) Additional Information: full citation, references, citings, index terms

5 Public protection of software

Amir Herzberg, Shlomit S. Pinter
October 1987 **ACM Transactions on Computer Systems (TOCS)**, Volume 5 Issue 4
Publisher: ACM Press
Full text available: pdf(1.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

One of the overwhelming problems that software producers must contend with is the unauthorized use and distribution of their products. Copyright laws concerning software are rarely enforced, thereby causing major losses to the software companies. Technical means of protecting software from illegal duplication are required, but the available means are imperfect. We present protocols that enable software protection, without causing substantial overhead in distribution and maintenance. The pro ...

6 Who's got the key?

David Henry
November 1999 **Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations SIGUCCS '99**
Publisher: ACM Press
Full text available: pdf(30.32 KB) Additional Information: full citation, references, index terms

Keywords: PKI, certificate authority, encryption

7 KHIP—a scalable protocol for secure multicast routing

Clay Shields, J. J. Garcia-Luna-Aceves
August 1999 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '99**, Volume 29 Issue 4
Publisher: ACM Press
Full text available: pdf(1.54 MB) Additional Information: full citation, abstract, references, citings, index terms

We present Keyed HIP (KHIP), a secure, hierarchical multicast routing protocol. We show that other shared-tree multicast routing protocols are subject to attacks against the multicast routing infrastructure that can isolate receivers or domains or introduce loops into the structure of the multicast routing tree. KHIP changes the multicast routing model so that only trusted members are able to join the multicast tree. This protects the multicast routing against attacks that could form branches to ...

8 Emperor: cheap legal secure cryptography for the Web

Clifton Davis, Christoph F. Eick
February 1999 **Proceedings of the 1999 ACM symposium on Applied computing SAC '99**
Publisher: ACM Press
Full text available: pdf(864.94 KB) Additional Information: full citation, references, index terms

Keywords: Web security, distributed source cryptography, electronic commerce, public key cryptography

9 Timestamps in key distribution protocols

Dorothy E. Denning, Giovanni Maria Sacco
August 1981 **Communications of the ACM**, Volume 24 Issue 8
Publisher: ACM Press
Full text available: pdf(397.16 KB) Additional Information: full citation, abstract, references, citings, index terms

The distribution of keys in a computer network using single key or public key encryption is discussed. We consider the possibility that communication keys may be compromised, and show that key distribution protocols with timestamps prevent replays of compromised keys. The timestamps have the additional benefit of replacing a two-step handshake.

Keywords: communications, encryption, encryption keys, key distribution, security, timestamps

10 Network security via private-key certificates

Don Davis, Ralph Swick
September 1990 **ACM SIGOPS Operating Systems Review**, Volume 24 Issue 4
Publisher: ACM Press
Full text available: pdf(256.46 KB) Additional Information: full citation, abstract, citings, index terms

We present some practical security protocols that use private-key encryption in the public-key style. Our system combines a new notion of *private-key certificates*, a simple key-translation protocol, and key-distribution. These certificates can be administered and used much as public-key certificates are, so that users can communicate securely while sharing neither an encryption key nor a network connection.

11 Securing ATM networks

Shaw-Cheng Chuang
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

12 Strong loss tolerance of electronic coin systems

Birgit Pfitzmann, Michael Waidner
May 1997 **ACM Transactions on Computer Systems (TOCS)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: Additional Information: full citation, abstract, references, citings, index

pdf(267.29 KB) terms, review

Untraceable electronic cash means prepaid digital payment systems, usually with offline payments, that protect user privacy. Such systems have recently been given considerable attention by both theory and development projects. However, in most current schemes, loss of a user device containing electronic cash implies a loss of money, just as with real cash. In comparison with credit schemes, this is considered a serious shortcoming. This article shows how untraceable electronic cash can be m ...

Keywords: Byzantine faults, electronic cash, payment systems, privacy

13 The Jupiter audio/video architecture: secure multimedia in network places

Pavel Curtis, Michael Dixon, Ron Frederick, David A. Nichols
January 1995 **Proceedings of the third ACM international conference on Multimedia MULTIMEDIA '95**
Publisher: ACM Press
Full text available: htm(72.37 KB) Additional Information: full citation, references, citings, index terms

Keywords: audio, collaboration, encryption, multicast, network places, security, video

14 Technical correspondence: file updating—still once more

Wesley Peterson
August 1981 **Communications of the ACM**, Volume 24 Issue 8
Publisher: ACM Press
Full text available: pdf(436.69 KB) Additional Information: full citation, references

15 Adding time to a logic of authentication

Paul F. Syverson
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(859.51 KB) Additional Information: full citation, abstract, references, citings, index terms

In [BAN89] Burrows, Abadi, and Needham presented a logic (BAN) for analyzing cryptographic protocols in terms of belief. This logic is quite useful in uncovering flaws in protocols; however, it also has produced confusion and controversy. Much of the confusion was cleared up when Abadi and Tuttle provided a semantics for a version of that logic (AT) in [AT91].In this paper we present a protocol to show that both BAN and AT are not expressive enough to capture all of the kinds of ...

16 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

17 Technical reports

SIGACT News Staff
January 1980 **ACM SIGACT News**, Volume 12 Issue 1
Publisher: ACM Press
Full text available: pdf(5.28 MB) Additional Information: full citation

18 Papers: Context-agile encryption for high speed communication networks
Lyndon G. Pierson, Edward L. Witzke, Mark O. Bean, Gerry J. Trombley
January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1
Publisher: ACM Press
Full text available: pdf(1.43 MB) Additional Information: full citation, abstract, references

Different applications have different security requirements for data privacy, data integrity, and authentication. Encryption is one technique that addresses these requirements. Encryption hardware, designed for use in high-speed communications networks, can satisfy a wide variety of security requirements if the hardware implementation is key-agile, key length-agile, mode-agile, and algorithm-agile. Hence, context-agile encryption provides enhanced solutions to the secrecy, interoperability, and ...

19 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

20 Symmetric and Asymmetric Encryption
Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 66 Result page: **1** 2 3 4 next